Master-Theorem

Master-Theorem I

Für $t(n) = a \cdot t(\frac{n}{b}) + g(n) \quad = \sum_{i=0}^{\log_b(n)} a^i \cdot g(\frac{n}{b^i})$
Mit $a > 0$, $b > 1$ und $g \in \Theta(n^c)$:

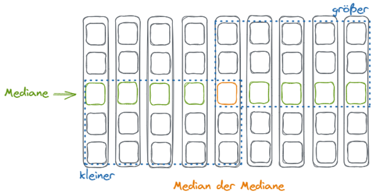
Fall 1	$a < b^c$	$t(n) \in \Theta(n^c)$
Fall 2	$a = b^c$	$t(n) \in \Theta(n^c \log(n))$
Fall 3	$a > b^c$	$t(n) \in \Theta(n^{\frac{\log a}{\log b}})$ bemerke : $\frac{\log a}{\log b} > c$

Master-Theorem II

$T(n) \leqslant \sum_{i=1}^{r} T(\alpha_i n) + \mathcal{O}(n) \qquad$ für $\sum_{i=1}^{r} \alpha_i < 1$
$\Rightarrow T(n) \in \mathcal{O}(n)$

Ultimate-Heapsort (Median in Linearzeit)

- Median aus 5 Elementen ($\frac{n}{5}$ viele Blöcke mit je 6 Vergleichen)
- Median der Mediane (rekursiv $\Rightarrow T(\frac{n}{5})$)



$T(n) = \frac{6}{5}n + T(\frac{n}{5}) + n + T(\frac{7}{10}n)$
n : Quicksort-Schritte
$\frac{3}{10}$ können durch Median ausgeschlossen werden
bemerke : $\frac{1}{5} + \frac{7}{10} < 1 \;\Rightarrow$ Master-Theorem II $\;\Rightarrow \mathcal{O}(n)$

Euklidischer Algo

größter gemeinsamer Teiler $\mathbf{ggT}(m, n)$
$\text{ggT}(n \mod m, m) = \text{ggT}(m, m)$

einfacher Euklid

Beispiel ggT(99, 78) :
$$\begin{aligned} \underline{99} &= 1 \cdot \underline{78} + \underline{21} \\ \underline{78} &= 3 \cdot \underline{21} + \underline{15} \\ \underline{21} &= 1 \cdot \underline{15} + \underline{\ 6} \\ \underline{15} &= 2 \cdot \underline{\ 6} + \underline{\ 3} \\ \underline{6} &= 2 \cdot \underline{\ 3} + \underline{\ 0} \end{aligned}$$

Sobald Rest $= 0$ ist der Divisor der ggT (hier 3).
Laufzeit max. $\frac{3}{2}\log_2 m$ Schritte

Erweiterter Euklidischer Algo

Lemma von Bézout : $\text{ggT}(m, n) = am + bn$
(ggT immer als Linearkombination darstellbar)

a	b	q	r	x	y
23	17	1	6	3	$-1 - 1 \cdot 3 = -4$
17	6	2	5	-1	$1 - 2 \cdot (-1) = 3$
6	5	1	1	1	$0 - 1 \cdot 1 = -1$
5	1	5	0	0	1

initial

$\text{ggT}(23, 17) = 1 = 23 \cdot 3 + 17 \cdot (-4)$

Einfachen Euklid ausführen. Danach Spalten x, y von unten füllen.
Initial ($x = 0$, $y = 1$). Danach :
$x_i = y_{i+1} \qquad$ und $\qquad y_i = x_{i+1} - (q_i \cdot y_{i+1})$

Wenn Multiplikative Inverse benötigt zB : $5 \cdot x \equiv 1 \mod 13$
$\Leftrightarrow 5x \mod 13 = 1 \implies 13a + 5b = 1$ mit erw. Euklid lösen

Restklassenring $\mathbb{Z}/n\mathbb{Z}$

beschreibt "Menge von Mengen".
Einheitsgruppe $(\mathbb{Z}/n\mathbb{Z})^* = \{k + n\mathbb{Z} \mid \text{ggT}(k, n) = 1\}$

Wichtigste Eigenschaften

$(k + n\mathbb{Z}) + (l + n\mathbb{Z}) = k + l + n\mathbb{Z}$ (Addition)
$(k + n\mathbb{Z}) \cdot (l + n\mathbb{Z}) = k \cdot l + n\mathbb{Z}$ (Multiplikation)
$\mathbb{Z}/n\mathbb{Z}$ ist Körper $\iff n$ ist prim

Chinesischer Restsatz

Für Teilerfremde Zahlen m, n :
Abbildung $\varphi : \; \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$
$\qquad x + mn\mathbb{Z} \mapsto (x + m\mathbb{Z}, x + n\mathbb{Z})$
ist Isomorphismus von Ringen.
Folgerung : unendlich viele Primzahlen

Kleiner Satz von Fermat

(Verallgemeinerung von Satz von Euler :
$\forall a, n \in \mathbb{N} : \text{ggt}(a, n) = 1 \implies a^{\varphi(n)} \equiv 1 \mod n$)
Für Primzahl p und $\forall a \in \mathbb{Z}$: $\quad a^p \equiv a \mod p$
Falls $p \nmid a$ (a kein Vielfaches von p) : $\quad a^{p-1} \equiv 1 \mod p$

Primzahltest (von n) nach Fermat
Wähle a $in\{1, ..., n-1\}$ zufällig.
Falls $a^{n-1} \mod n \not\equiv 1 \mod n \implies$ n KEINE Primzahl

Modulo-Tricks

- Satz von Euler (für Exponenten) & Chin. Restsatz (für Modul)
- mod 3 ist Quersumme mod 3 (mod in Summe $\sum a_i \cdot 10^i$ ziehen)
- binäre Exponentiation
- $x^d \mod n \Leftrightarrow x^{d \mod (p-1)} \mod p \wedge x^{d \mod (q-1)} \mod q$ mit p, q prim, $n = pq$
- "-1"-Trick

RSA

Primzahlen p und q, $p < q$. Damit $n = p \cdot q$, $\varphi(n) = (p-1)(q-1)$
Wähle $e > 0$ mit $\text{ggT}(e, \varphi(n)) = 1$ (Euklidischer Algo)
Berechne d : $\; e \cdot d \equiv 1 \mod \varphi(n) \quad d < n$
$\qquad \Leftrightarrow e \cdot d \mod \varphi(n) = 1$ bzw. $d = e^{-1} \mod \varphi(n)$
$E(x, (n, e)) = x^e \mod n \qquad (n, e) \in K_{\text{pub}}$
$D(y, (n, d)) = y^d \mod n \qquad (n, d) \in K_{\text{priv}}$

Eulers φ-Funktion

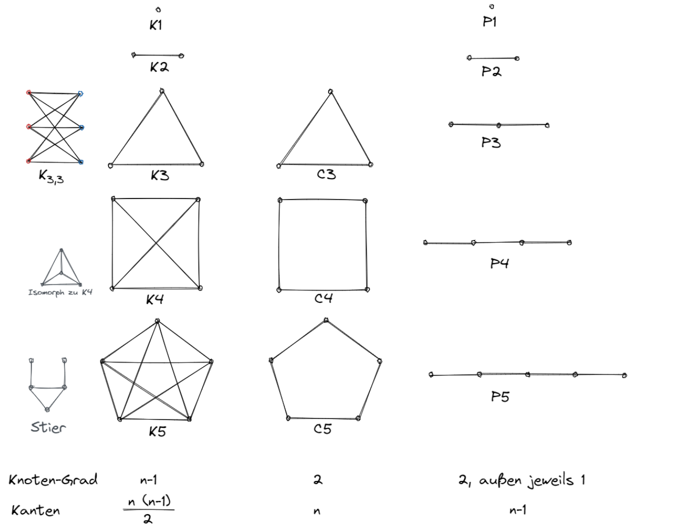
$\varphi(n) = |\{k < n : \; \text{ggT}(k, n) = 1\}|$
Anzahl ganzer teilerfremde Zahlen unter n.
Für prim : $\varphi(p) = (p-1)$ und $\varphi(p^e) = p^{e-1}(p-1) = p^e - p^{e-1}$

Primzahldichte

$\pi(n)$ Anzahl Primzahlen bis ink. $n \qquad \pi(n) \geqslant \frac{n}{\log_2 n}$
$\frac{n}{\log_2 n} \leqslant \pi(n) \leqslant \frac{(2+\epsilon)n}{\log_2 n}$
Bertrand'sches Postulat $\forall n \geqslant 1 : \; \exists p$ prim : $\; n < p \leqslant 2n$

Ungerichtete Graphen $G = (V, E)$

V, E : Mengen von Knoten, Kanten. $E \subseteq \binom{V}{2}$



bipartit : Knotenmenge V kann in zwei aufgeteilt werden, so dass keine Kante zwei Knoten der gleichen Menge verbindet. Bsp : $K_{3,3}$
d(u) : Grad (degrees)
Summe aller Knotengrade ist gerade (ungerichteter Graph).
Anzahl Knoten mit ungeradem Grad ist gerade!
(Perfect) Matching : So Kanten wählen, dass jeder Knoten mit max. einem anderen Knoten verbunden ist.
Perfect, wenn alle Knoten beteiligt.
Unabhängige Menge : Knoten, die nicht verbunden sind.

Clique

Graph G, $V' \subseteq V$ ist Clique, falls $\forall u, v \in V'$: $\; u \neq v \;\Rightarrow\; (u, v) \in E$

Satz von Ramsey

$\forall n : \; \exists N$: Jeder Graph mit N Knoten hat entweder
(eine Clique oder unabhängige Menge) der Größe n
Ramsey-Zahl $R(n)$ für kleinsten Graph N

Planar

Isomorpher G. auf Ebene ohne kreuzende Kanten existiert.
G ist planar $\Leftrightarrow$ G enthält keine Unterteilung von K_5 oder $K_{3,3}$
~Satz von Kuratowski

Eulerformel

$n - m + f = 2 \qquad$ n Knoten, m Kanten, f Facetten (+1 Außen).
für endliche, zusammenhängende, planare Graphen. $n \geqslant 1$
Mind. 3 Kanten pro Facette, jede Kante max. 2 Facetten : $3f \leqslant 2m$
$4f \leqslant 2m$ bei bipartiten Graphen

Wege und Kreise

Länge von Weg : Kanten!
Euler'scher Weg : Jede Kante einmal in Pfad (max. 2 Knoten mit ungeradem Grad)
Euler'scher Kreis : Anfangsknoten = Endknoten (jeder Knoten gerader Grad)
Hamilton'scher Weg : Jeder Knoten einmal

Sortieralgos

Da entscheidungsbasiert : mind. Laufzeit von $\log(n!) \in \Omega(n \log n)$.
Algo durchquert Baum mit $n!$ Blättern.

Dykstra

Setzte Kosten aller Knoten auf ∞, außer Startknoten (hier 0).
Füge alle Knoten in eine Queue.
Wähle Konten mit kleinstem Wert.
-> Setzte Kosten aller ausgehend verbundenen Knoten auf :
Eigene Kosten + Kosten des Pfades (Wenn niedriger, als die aktuellen)
WIEDERHOLE, bis Queue leer ist.
Beweisbar optimal, Greedy

Bekannte Laufzeiten

Algo	Worst-Case	Average-Case
Quicksort	$\mathcal{O}(n^2)$	$2n \ln n < 1.4n \log n$
Heapsort	$2n \log n + \mathcal{O}(n)$	$2n \log n + \mathcal{O}(n)$
Bottom-up Heapsort	$1.5n \log n + o(n \log n)$	$n \log n + o(n \log n)$

CYK-Algo

Länge	w1	w2	...
1	T1,1	T2,1	...
2	T2,1	T2,2	
...			

$T_{i,j} = \{A \in V | A \Rightarrow_G^* a_i ... a_{i+j-1}\}$

Algo optimale Klammerung

Ähnlich zu CYK. $T_{i,j} = \min_{i \leqslant m < j}(T_{i,m} + T_{m+1,j} + n_{i-1} \cdot n_m \cdot n_j)$
Benutzte Technik : Memoization (dyn. Programmieren)

Wachstum

Landau-Symbole

$f \in o(g)$: $\prec$ f wächst langsamer als g
$f \in \mathcal{O}$: $\preceq$ f wächst nicht (wesentlich) schneller als ...
$f \in \Theta$: $\asymp$ f wächst genauso schnell wie ..
$f \in \Omega$: $\succeq$ f wächst nicht (wesentlich) langsamer als ..
$f \in \omega$: $\succ$ f wächst schneller als ..
Beweis $f(n) \in \mathcal{O}(b(n))$: $\exists c \exists n_0 \ \forall (n \geqslant n_0)$: $b(n) \leqslant c \cdot f(n)$

Bekannte Relationen

$\log(n!) \in \Omega(n \log n)$ (Worst-Case vergleichsbasiertes Sortieren)
$\Theta(1) < \Theta(\log \log n) < \Theta((\log \log n)^2) < \Theta(\log n) < \Theta(\sqrt{n}) < \Theta(n) < \Theta(n \cdot \log n) < \Theta(n^2) < \Theta(2^n) < \Theta(n!) < \Theta(n^n) < \Theta(2^{n^2})$

von $n!$ (für $n \geqslant 2$)

$(\frac{n}{2})^{\frac{n}{2}} < n! < n^n$
$\log(n!) \in \Theta(n \log n)$
$e \cdot (\frac{n}{e})^n \leqslant n! \leqslant n \cdot e \cdot (\frac{n}{e})^n$
$n! \approx \sqrt{2\pi n} \cdot (\frac{n}{e})^n$ (Stirling-Formel)

von Binomialkoeffizient $\binom{n}{k}$

Maximal bei $\binom{2n}{n}$ bzw. $\binom{n}{\lfloor \frac{n}{2} \rfloor} = \binom{n}{\lceil \frac{n}{2} \rceil}$
$\sum_k \binom{n}{k} = 2^n$ da alle Möglichkeiten.
$\binom{n}{\lfloor \frac{n}{2} \rfloor} = \binom{n}{\lceil \frac{n}{2} \rceil} > \frac{2^n}{n}$ für $n \geqslant 3$
Durchschnittswert $\binom{n}{k}$ ist $\frac{2^n}{n}$

kgV(n) - Kleinstes gemeinsames Vielfaches

$\text{kgV}(n) = \text{kgV}(2, ..., n)$
$\text{kgV}(5, 8) = 40$, da Primfaktorzerlegung $5 = 5$, $8 = 2 \cdot 2 \cdot 2$.
Alle P-faktoren in ihrer höchsten Anzahl zusammenfassen und aufmultiplizieren.
$2^{n-1} < \text{kgV}(n) \leqslant n!$
$2^n < \text{kgV}(n) \leqslant 4^{n-1}$ für $n \geqslant 7$
$m \cdot \binom{n}{m}$ teilt $\text{kgV}(n)$

Kombinatorik / Stochastik

Zufallsvariable X : $\Omega \mapsto \mathbb{R}$
X, Y sind unabhängig, wenn :
$\mathbb{P}(X = x \wedge Y = y) = \mathbb{P}(X = x) \cdot \mathbb{P}(Y = y)$
Erwartungswert $\mathbb{E}(X) = \sum_{\omega \in \Omega} X(\omega) \cdot \mathbb{P}(\omega)$
Varianz $\mathbb{V}(x) = \mathbb{E}((X - \mathbb{E}(X))^2) = \mathbb{E}(X^2) - \mathbb{E}(X)^2$

Bedingte Wahrscheinlichkeit

$\mathbb{P}(B|A) = \frac{\mathbb{P}(B \cap A)}{\mathbb{P}(A)}$
$\mathbb{P}(A|B) = \frac{\mathbb{P}(B|A)\mathbb{P}(A)}{\mathbb{P}(B)}$ Satz von Bayes

Markov-Ungleichung

$\forall \lambda > 0 :\ \mathbb{P}(X \geqslant \lambda \cdot \mathbb{E}(X)) \leqslant \frac{1}{\lambda}$ für $\mathbb{E}(X) > 0$, X ist ZV.

Anzahl Ergebnisse

Ziehe k aus n Optionen :

		Zurücklegen	
		Ja	Nein
Reihenfolge	Ja	n^k	$\frac{n!}{(n-k)!} = \binom{n}{k} \cdot k! = n^{\underline{k}}$
	Nein	$\binom{n+k-1}{k}$	$\binom{n}{k}$

Binomialverteilung

$\mathbb{P}(X = k) = \binom{n}{k} \cdot p^k \cdot (1-p)^{n-k}$
$\mathbb{E}(X) = n \cdot p$, $\mathbb{V}(X) = n \cdot p \cdot (1-p)$

Geometrische Verteilung *(Wartezeitprobleme)*

$\mathbb{P}(X = k) = p \cdot (1-p)^k$ (erfolg im k-ten Versuch)
$\mathbb{E}(X) = \frac{1-p}{p}$, $\mathbb{V}(X) = \frac{1-p}{p^2}$

Nice to knows

Isomorphismus

ist ein bijektiver **Homomorphismus :**
strukturerhaltende Abbildung :
$\varphi : (M_1, \circ_1, e_1) \mapsto (M_2, \circ_2, e_2)$ mit $\varphi(m \circ_1 m') = \varphi(m) \circ_2 \varphi(m')$

Primzahlzertifikat für n

$\forall$ Primzahlen p : $n \equiv 1 \mod p$: $\exists a \in \mathbb{Z}$:
$a^{n-1} \equiv 1 \mod n$ und $a^{\frac{n-1}{p}} \not\equiv 1 \mod n$

Reihen

$\sum_{k=1}^n q^k = \frac{1-q^{n+1}}{1-q}$ geom. Teil-Reihe
$\sum_{k=1}^\infty q^k = \frac{1}{1-q}$ für $|q| < 1$ geom. Reihe
$\sum_{k=1}^\infty kq^{k-1} = \frac{1}{(1-q)^2}$ für $|q| < 1$ geom. Reihe abgeleitet
$\sum_{k=1}^n k = \frac{n(n+1)}{2}$ gaußsche Summenformel
Harmonische Zahl $H_n = \sum_{i=1}^n \frac{1}{i} \approx \ln(n)$ $\ln n \leqslant H_n \leqslant \ln n + 1$

Logarithmus-Regeln

$\log(x \cdot y) = \log x + \log y$ | $\log x^n = n \cdot \log x$
$\log_a x = \frac{\log_b x}{\log_b a}$ | $a^{\log(b)} = b^{\log(a)}$

Binomialkoeffizienten

Wie viele k-elementige Teilmengen existieren von $[n]$?
$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \binom{n-1}{k} + \binom{n-1}{k-1}$
$\binom{n}{0} = \binom{n}{n} = 1$ und $\binom{n}{1} = \binom{n}{n-1} = n$
$\binom{n}{k} = \binom{n}{n-k}$ (symetrisch)

Satz von Wilson

$(n-1)! \equiv -1 \mod n \Leftrightarrow n$ ist Primzahl

Fibonacci-Zahlen

$F_0 = 0,\ F_1 = 1,\ F_{n+2} = F_{n+1} + F_n$
$F_n \leqslant 2^n \leqslant F_{2n}$ oder $(\sqrt{2})^n \leqslant F_n \leqslant 2^n$
$\text{ggT}(F_m, F_n) = F_{\text{ggT}(m,n)}$

Partitionszahlen

n Elemente $\rightarrow$ k nichtleere Teilmengen aufteilen. Reihenfolge egal.
$P(n,k) = P(n-1, k-1) + P(n-k, k)$
$P_{7,3} = 4$, da $7 = 1+1+5 = 1+2+4 = 1+3+3 = 2+2+3$

Catalanzahlen

$C_n = \frac{1}{n+1}\binom{2n}{n} = \frac{1}{2n+1}\binom{2n+1}{n}$ | $C_1 = 1, C_2 = 2, C_3 = 5, C_4 = 14$
$C_n \sim \frac{4^n}{n \cdot \sqrt{\pi n}}$ (durch Stirling)
C_n gibt Anzahl saturierter Binärbäume mit n inneren Knoten an ($n+1$ Blätter)

Dyck-Wörter (Klammerwörter)

a : "(" b : ")"
D_n Menge an Dyck-Wörtern mit Länge $2n$ (also n Klammern)
$w \in D_n$ wenn $|w|_a = |w|_b \wedge (\forall w_{\text{prefix}}$ aus w : $|w_{\text{pref}}|_a \geqslant |w_{\text{pref}}|_b)$
$|D_n| = C_n$ für $n \geqslant 1$

Induktion

IA, IV & IS.
Für starke Induktion : IV für $m = 1, 2, ..., n$

Algebraische Strukturen

Magma : binäre Verknüpfung $\circ : S \times S \mapsto S$
Halbgruppe : $\circ$ assoziativ : $(x \circ y) \circ z = x \circ (y \circ z)$
Monoid : $(S, \circ)$: $\exists$ neutrales Element e : $\forall x \in S : x \circ e = x = e \circ x$
Gruppe : Jedes Element hat Inverses : $x \circ x^{-1} = e = x^{-1} \circ x$
Alle können kommutativ sein $(x \circ y = y \circ x)$ (gilt nicht für Minus)
Äquivalenzklasse : $[x]_\sim = \{y \in M | x \sim y\}$ bezogen auf Monoid $(M, \circ)$ mit Äquivalenzrelation $\sim$
Quotientenmenge : $M/\sim = \{[x]_\sim \mid x \in M\}$
Kongruenzrelation falls : $x \sim x' \wedge y \sim y' \Rightarrow x \circ y \sim x' \circ y'$